PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00

A2

(11) International Publication Number: **WO 00/26746**

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/EP99/08331

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:
198 50 721.6 3 November 1998 (03.11.98) DE

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: THÜRINGER, Peter [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). ULLY, Klaus [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). ARNOLD, Siegfried [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). EBER, Wolfgang [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Agent: SCHMALZ, Günther; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(81) Designated States: CN, JP, KR, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: DATA CARRIER WITH OBSCURED POWER CONSUMPTION

(57) Abstract

In order to prevent the retrieval of data via the measurement of the power consumption in a data carrier provided with a data processing device, it is proposed to connect a load circuit to the power supply of the data carrier so as to influence the power consumption of the data carrier at least during security–relevant operations of the data processing device.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Data carrier with obscured power consumption.

The invention relates to a data carrier with a data processing device as well as to an electronic component with a data processing device, for example for such a data carrier.

Recently doubts have been raised as regards the security of data carriers, it being stipulated that security-relevant data could be determined by monitoring the power consumption of such data carriers. It is true that during all logic operations, so also during sensible operations or sub-operations (for example cryptographic calculations) current power is consumed by switching operations in the logic circuitry in dependence on the result or logic level. Measurement of the power consumed by the circuit, therefore, could be used for an attack so as to find out secret data (key) by means of mathematical methods (correlations, power analysis).

It is an object of the invention to prevent such attempts from being successful.

This object is achieved in that a load circuit is connected to the power supply of the data carrier and is intended to influence the power consumption of the data carrier at least during security-relevant operations of the data processing device.

The power consumption that can be measured externally thus no longer corresponds to the power consumption of the data processing device alone, but also contains a further component which preferably is not directly related to the internal operations of the data processing device.

A particularly simple embodiment is obtained when the load circuit is constructed as a variable ballast resistor which in the simplest case may consist of a transistor or a network of series and parallel-connected transistors, connected to the same power supply lead in parallel with the data processing device. Different load states can be adjusted by appropriate control of the load resistor or load resistors.

A more complex embodiment is provided with a circuit arrangement which is constructed so as to be complementary to at least parts of the data processing device and can be controlled in parallel with the data processing device. Changes in the switching state, initiated during security-relevant operations, are thus carried out in a complementary fashion at the same time. Even if the power consumption should be different for different logic levels, in the ideal case the power consumption is constant because of the complementary switching

states. However, because it cannot be detected from the outside what power consumption relates to the logic states actually involved in the security-relevant operations and what power consumption is involved in the complementary switching states which occur in parallel merely for the purpose of masking, it is not even necessary to pursue a constant power consumption. Therefore, it is not even necessary to construct all switching circuit components required for the security-relevant operations in a complementary fashion, but it suffices to make only a part of the circuit components complementary.

Preferably, the load circuit and the data processing device are integrated in a common circuit because the separation of the load circuit from the data processing data for the purpose of attempted discovery requires far more technical means than when these circuit components are arranged on the data carrier in a physically separated manner. The analysis of circuit elements actually involved in security-relevant operations is rendered more complicated notably when the circuit elements required are physically mixed with complementary circuit elements in one chip.

The invention will be described in detail hereinafter.

The invention is used, for example in so-called chip cards 1 or integrated circuits 3 (chip card chips) for such chip cards. Different constructions (for example SIM card, secure access model for a terminal, contactless or dual interface transponders) are feasible, the power supply being possible via contacts 2, in a contactless manner, for example by induction of alternating current, or also by means of internal power supply sources such as rechargeable batteries. Therefore, the invention is suitable for any type of power supply. If the invention is incorporated in the relevant chip, usable information cannot be extracted either by a deliberate attempt aimed at the power supply provided within a chip card.

Fig. 1 shows such a chip card 1 with an embedded chip 3 which is connected to a contact field 2 by internal wires 4.

Generally speaking, it would also be possible to construct all logic elements of a chip as a complementary copy. As an example for all logical elements of a chip Fig. 2 shows a first AND-gate 5. The inputs of this AND-gate 5 are connected, via logic inverters 6, 7, to a second AND-gate 8 which forms the complementary gate and acts as a supplementary load. Preferably, delay elements are inserted in the input lines of the first AND-gate 5 in order to compensate the signal delay of the inverters 6, 7. As the output of the first AND-gate 5 switches to logic "1" when both of its inputs are logic "1" and the output of the second AND-gate 8 switches to "1" when the inputs of the first AND-gate are all of logic value "0", it cannnot be recognized from outside if switching occurs when all the inputs of the first AND-

gate 5 are set to "0" or are set to "1" If a third and a fourth AND-gate were added parallel to the first and second AND-gate with a single inverter connected in-between one of the inputs, exactly one of those four AND-gates would switch every time when one of the logic values of the inputs changes. Because chips in a chip card are exposed to mechanical loads, however, they should not exceed a given size. Therefore, it is considered to be sufficient if only the logic elements which execute sensitive operations are constructed so as to be complementary. Two alternatives seem to be attractive for copying. On the one hand, security-relevant circuit elements, being of interest to a fraud because of the power consumption, can actually be provided on the chip in complementary logic so as to be controlled in parallel. For example, if during the calculation of a cryptogram, during which a secret in the form of a key which is unknown to the fraud is input, a logic level becomes high on a node at a given instant, be it random during the calculation (the previous state may have been low or high), in the complementary logic the state low is generated at the comparable node (the immediately previous state was high or low).

Consequently, for sensitive operations the number of low-high transitions and the number of high-low transitions are exactly equal and the number of nodes which are high at a given instant corresponds exactly to the number of nodes which are low. The surface area required by the complementary logic corresponds exactly to the surface area required by the copied logic.

On the other hand, it is also possible to realize a complementary machine which copies all logic combinations, be it not identical, by the switching of different load states.

Fig. 3 shows a complementary machine 10 which is connected, via wires 10, to nodes of security-related circuit elements of parts 9 of the chip performing the calculation of the cryptogram. In relation to the states of the sensored nodes, the complementary machine 10 calculates an appropriate load and switches, via switching transistors 12, the calculated number of load resistors 13.

This step is aimed at the generating of a power consumption which is independent of the data or the key but not necessarily constant, in order to achieve resistance against attacks which utilize the power consumption as a starting point (simple or differential power analysis). In any case the object is not to achieve a constant power consumption of the circuit by complex control concepts.

This concept can be realized independently of the construction of the logic (synchronous or asynchronous circuit technique).

CLAIMS:

1. A data carrier which includes a data processing device, characterized in that a load circuit which is connected to the power supply of the data carrier is provided so as to influence the power consumption of the data carrier at least during security-relevant operations of the data processing device.

2. A data carrier as claimed in claim 1, characterized in that the load circuit is formed by a variable load resistor.

3. A data carrier as claimed in claim 1, characterized in that a circuit arrangement which is constructed so as to be complementary to at least parts of the data processing device can be controlled in parallel with the data processing device.

4. A data carrier as claimed in claim 1, characterized in that the load circuit is constructed so as to be controllable by way of its own logic which is intended to generate a load state which is complementary to the power consumption of the data processing device.

5. An electronic component, notably an integrated component provided with a data processing device, characterized in that a load circuit which is internally connected to the power supply of the electronic component is arranged to influence the power consumption of the electronic component at least during security-relevant operations of the data processing device.

6. An electronic component as claimed in claim 5, characterized in that the load circuit consists of a variable load resistor.

7. An electronic component as claimed in claim 5, characterized in that the load circuit is formed by a circuit arrangement which is constructed so as to be complementary with at least parts of the data processing device and can be controlled in parallel with the data processing device.

8. An electronic component as claimed in claim 5, characterized in that the load circuit can be controlled by means of its own logic which is arranged to produce a load state which is complementary to the power consumption of the data processing device.

1/1

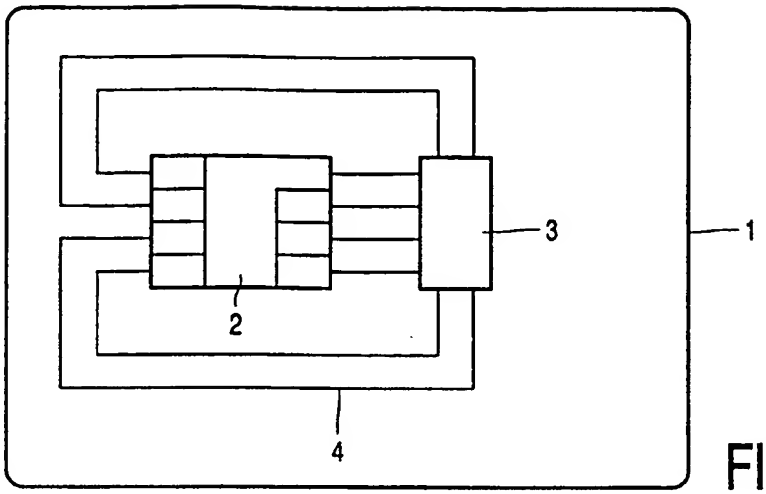

FIG. 1

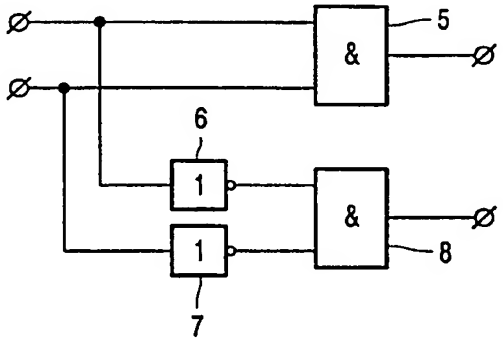

FIG. 2

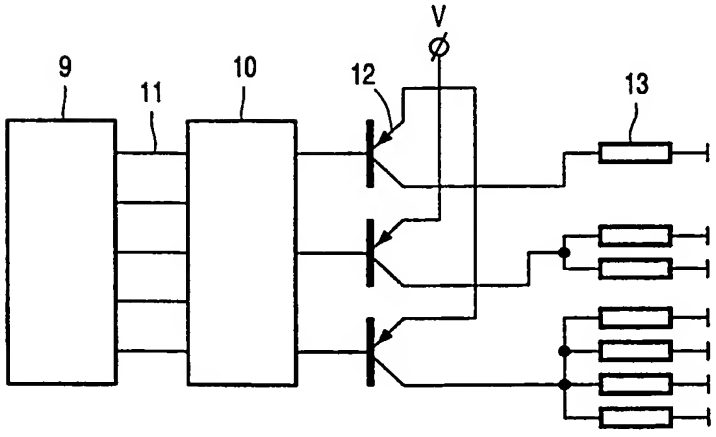

FIG. 3

INTERNATIONAL SEARCH REPORT

Inte: onal Application No
PCT/EP 99/08331

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G11C7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) abstract; figure 1 column 3, line 26 - line 57 column 4, line 12 - line 26 claims 1-9	1,2,5,6
Y		3,4,7,8
Y	US 5 500 601 A (FOURNEL RICHARD ET AL) 19 March 1996 (1996-03-19) abstract; figure 2 claims 1-11	3,4,7,8
A	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 March 1989 (1989-03-14)	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 2000	17/05/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter nal Application No
PC./EP 99/08331

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
US 5500601 A	19-03-1996	FR 2673295 A	28-08-1992
		DE 69220979 D	28-08-1997
		DE 69220979 T	12-02-1998
		EP 0500461 A	26-08-1992
US 4813024 A	14-03-1989	FR 2600183 A	18-12-1987
		DE 3777701 A	30-04-1992
		EP 0251853 A	07-01-1988
		JP 63080351 A	11-04-1988